

Appl. No. 09/622,047
Reply to Office Action of Nov. 9, 2004 and Feb. 23, 2005

Attorney Docket: P65855US0

REMARKS

In the Advisory Action of February 23, 2005, the Examiner indicated that the rejection under 35 U.S.C. 112 first paragraph has been overcome. In this Amendment, Applicant has amended Claim 1 to specify the embodiments of the present invention and overcome the pending rejections. It is respectfully submitted that no new matter has been introduced by the amended claims. All claims are now present for examination and favorable reconsideration is respectfully requested in view of the preceding amendments and the following comments.

REJECTIONS UNDER 35 U.S.C. § 102:

Claim 1 has been rejected under 35 U.S.C. § 102 (e) as allegedly being anticipated by Den Boer et al. (US 6,298,136), hereinafter Den Boer.

Applicant traverses the rejection and respectfully submits that the present-claimed invention is not anticipated by the cited reference. More specifically, the embodiment of the present invention as defined in the amended Claim 1 includes the feature of "transforming the subkey with the operation of transposing bits, which changes initial sequence of the subkey bits and depends on the j-th subblock prior to performing the two-place operation on the i-th subblock, where $i \neq j$." Such feature is not disclosed or taught by Den Boer.

As previously pointed out, Den Boer does not disclose the conversion of data subblocks which are then used to convert subkeys. The description at col. 4, lines 35 – 56 of Den Boer does not support such conclusion. The term "third input block 450" means a device for receiving the key and not data blocks to be converted, as evidenced also by the fact that Den Boer calls data blocks "digital input blocks" (lines 40-41, 45, 47, 48, 50, 51, 53, 59, 60), "digital output block" (in lines 46, 47, 49, 51, 55, 63), "data block" (line 53).

Appl. No. 09/622,047
Reply to Office Action of Nov. 9, 2004 and Feb. 23, 2005

Attorney Docket: P65855US0

In addition, Den Boer fails to disclose the feature of "transforming the subkey with the operation of transposing bits, which changes initial sequence of the subkey bits and depends on the j-th subblock prior to performing the two-place operation on the i-th subblock, where $i \neq j$."

Therefore, the newly presented claim is not anticipated by Den Boer and the rejection under 35 U.S.C. § 102 (e) has been overcome. Accordingly, withdrawal of the rejection under 35 U.S.C. § 102 (e) is respectfully requested.

REJECTIONS UNDER 35 U.S.C. § 103:

Claims 2 – 4 have been rejected under 35 U.S.C. § 103 as allegedly being unpatentable over by Den Boer, in view of Coppersmith et al. (US 6,192,129), hereinafter Coppersmith.

Applicant traverses the rejection and respectfully submits that the embodiments of present-claimed invention are not obvious over Den Boer, in view of Coppersmith. As stated above, Den Boer does not disclose the invention as amended. Similarly, Coppersmith also fails to teach or suggest the embodiments of the present invention as defined in Claims 2 – 4, especially the feature of "transforming the subkey with the operation of transposing bits, which changes initial sequence of the subkey bits and depends on the j-th subblock prior to performing the two-place operation on the i-th subblock, where $i \neq j$." In Coppersmith, round subkeys are generated according to a determined law. Therefore, during the encryption of various data blocks, the value of subkeys remains unchanged over a preset conversion step of some preset round in the encryption methods described in Coppersmith. In addition, as admitted by the Examiner, Den Boer does not expressly disclose either an operation of permuting subkey bits or a substitute operation performed on a subkey as being the conversion operation step. Therefore, there is no motivation to combine Den Boer and Coppersmith. Even if they are combined, Den Boer and Coppersmith will not render the present claimed invention

Appl. No. 09/622,047
Reply to Office Action of Nov. 9, 2004 and Feb. 23, 2005

Attorney Docket: P65855US0

obvious. One of ordinary skill in the art would not discern the present invention as claimed at the time of its invention.

Therefore, the newly presented claims are not anticipated by Den Boer and Coppersmith and the rejection under 35 U.S.C. § 103 has been overcome. Accordingly, withdrawal of the rejections under 35 U.S.C. § 103 is respectfully requested.

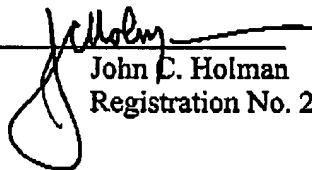
Having overcome all outstanding grounds of rejection, the application is now in condition for allowance, and prompt action toward that end is respectfully solicited.

Respectfully submitted,

JACOBSON HOLMAN PLLC

Date: May 5, 2005
(202) 638-6666
400 Seventh Street, N.W.
Washington, D.C. 20004
Atty. Dkt. No.: P65855US0

By



John C. Holman
Registration No. 22,769